Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-4. (Cancelled).

5. (Currently Amended) A ~~The~~ cryptographic communication system ~~as set forth in claim 4,~~ which permits a plurality of entities to mutually perform an encryption process for encrypting a plaintext as information to be transmitted into a ciphertext and a decryption process for decrypting the transmitted ciphertext into the original plaintext, the system comprising:

a plurality of key generating agencies, each of which generates a secret key of each entity by using each of divided identification information obtained by dividing identification information of each entity into a plurality of blocks and a hash value which consists of a plurality of bits and is set for each of the key generating agencies and sends the generated secret key to each entity; and

a plurality of entities, each of which generates a common key for use in the encryption process and decryption process by using components corresponding to an entity to be communicated with, contained in its own secret keys sent from the key generating agencies, respectively,

wherein the hash value is set for each of the key generating agencies, by selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits, and

wherein, when a new key generating agency is added to a plurality of existing key generating agencies, a hash value is set for the new key

generating agency by selecting a plurality of bits of any order from an original hash-value sequence consisting of a sequence of hash values set for the existing key generating agencies.

6-7. (Cancelled).

8. (New) A method of permitting a plurality of entities to mutually perform an encryption process for encrypting a plaintext as information to be transmitted into a ciphertext and a decryption process for decrypting the transmitted ciphertext into the original plaintext, the method comprising:

generating a secret key for a plurality of key generating agencies by dividing identification information of each entity into a plurality of blocks and setting a hash value which consists of a plurality of bits for each of the key generating agencies and sending the generated secret key to each entity; and

generating a common key for a plurality of entities for use in the encryption process and decryption process by using components corresponding to an entity to be communicated with, contained in its own secret keys sent from the key generating agencies, respectively,

wherein setting the hash value for each of the key generating agencies is provided by selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits, and

wherein, when a new key generating agency is added to a plurality of existing key generating agencies, setting a hash value for the new key generating agency is provided by selecting a plurality of bits of any order from an original hash-value sequence consisting of a sequence of hash values set for the existing key generating agencies.